

### REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-5, 7-11, and 13-27 are currently pending. Claims 6 and 12 have been cancelled without prejudice; Claims 1, 2, 4, 5, 7, 8, 10, 11, and 13 have been amended; and Claims 14-27 have been added by the present amendment. The changes and additions to the claims are supported by the originally filed specification and do not add new matter.

In the outstanding Office Action, Claims 1-13 were rejected under 35 U.S.C. § 101 as being directed to nonstatutory subject matter; and Claims 1, 2, 4-8, and 10-13 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,194,090 to Muratani et al. (hereinafter “the ‘090 patent”).<sup>1</sup>

Applicants respectfully submit that the rejections of Claims 1-6 under 35 U.S.C. § 101 are rendered moot by the present amendment to Claim 1. Claim 1 has been amended to recite a processor, and is thus not directed to software *per se*.

Applicants respectfully submit that the rejection of Claim 7 under 35 U.S.C. § 101 is rendered moot by the amendment to Claim 7. Claim 7 has been amended to be directed to a cryptographic processing method implemented by a cryptographic processing device configured to perform Feistel-type common-key-block cryptographic processing, wherein the method includes the steps of executing, by the cryptographic processing device, an SPN-type F-function for performing nonlinear conversion processing and linear conversion processing repeatedly over a plurality of rounds. Thus, Applicants respectfully submit that Claim 7 is tied to a particular machine, i.e., the cryptographic processing device. Accordingly,

---

<sup>1</sup> Applicants note that Claims 3 and 9 were not specifically rejected over the ‘090 patent or any other cited references. Accordingly, Applicants assume that Claims 3 and 9 would be allowable if amended to be in independent form and the rejections under 35 U.S.C. § 101 are overcome.

Applicants respectfully submit that Claim 7 satisfies the machine-or-transformation test set forth in *In re Bilski*, and is directed to statutory subject matter.

Applicants respectfully submit that the rejection of Claim 13 under 35 U.S.C. § 101 is rendered moot by the present amendment to Claim 13. Claim 13 has been amended to be directed to a computer readable medium storing a program, which when executed by a computer, causes the computer to perform Feistel-type common-key-block cryptographic processing. Accordingly, Applicants respectfully submit that the rejection is rendered moot.

Amended Claim 1 is directed to a cryptographic processing apparatus for performing Feistel-type common-key-block cryptographic processing, comprising: a processor that repeatedly executes an SPN-type F-function having a nonlinear conversion section and a linear conversion section over a plurality of rounds, wherein each of the linear conversion sections of an F-function corresponding to each of the plurality of rounds is configured to perform linear conversion processing of an input of  $n$  bits outputted from each of  $m$  nonlinear conversion sections, in total  $mn$  bits, as linear conversion processing that applies a square MDS (Maximum Distance Separable) matrix, at least in consecutive odd-numbered rounds and in consecutive even-numbered rounds, different square MDS matrices  $L_a$ ,  $L_b$  are applied, and a matrix composed of  $m$  row vectors selected arbitrarily from row vectors constituting inverse matrices  $L_a^{-1}$ ,  $L_b^{-1}$  of the square MDS matrices is linearly independent. The changes to Claim 1 are supported by the originally filed specification and do not add new matter.<sup>2</sup>

The '090 patent is directed to an encryption apparatus based on a common key encryption system in which a plurality of expanded keys are used in a predetermined order in a data randomizing process for encryption, the apparatus including a plurality of round processing circuits connected in series, the round processing circuit of a first stage receiving a common key and subjecting the received common key to a round function to output a sub-

---

<sup>2</sup> See, e.g., Figure 15 and the discussion related thereto in the specification.

key; and a plurality of expanded key generating circuits configured to receive the sub-keys output from at least a part of the round processing circuits and output expanded keys based on all or some bits of the received sub-keys.<sup>3</sup>

However, Applicants respectfully submit that the '090 patent fails to disclose that a matrix composed of m row vectors selected arbitrarily from row vectors constituting inverse matrices  $L_a^{-1}$ ,  $L_b^{-1}$  of the square MDS matrices is linearly independent, as required by amended Claim 1. In this regard, Applicants note that the Office Action cites to Figure 20, column 17, lines 36-46, and column 18, lines 6-13 in the '090 patent as disclosing this limitation. However, Applicants note that the passage in column 17 merely notes that several bits of the expanded keys at the last stage can only be specified, and that there is no problem with safety even in the simple Feistel structure shown in Figure 20. Further, the passage in column 18, lines 6-13 refers to Figure 24, which illustrates an encryption apparatus having a 128-bit block cipher and a common key having 256 bits.

However, Applicants note that the cited passages in columns 17 and 18 are silent regarding the linear independence of any matrices. In particular, the passages are silent regarding a matrix composed of m row vectors selected arbitrarily from row vectors constituting the inverse matrices  $L_a^{-1}$ ,  $L_b^{-1}$  of the square MDS matrices being linearly independent, as required by amended Claim 1. In particular, Applicants respectfully submit that the '090 patent is silent regarding any type of linear independence of matrices.

Thus, for the reasons stated above, Applicants respectfully submit that the rejection of Claim 1 is rendered moot by the present amendment to that claim.

Independent Claims 7 and 13 recite limitations analogous to the limitations recited in Claim 1, and have been amended in a manner analogous to the amendment to Claim 1. Accordingly, for the reasons stated above, Applicants respectfully submit that the rejections

---

<sup>3</sup> See, e.g., Figure 24 of the '090 patent.

of Claims 7 and 13 (and all associated dependent claims) are rendered moot by the present amendment to Claims 7 and 13.

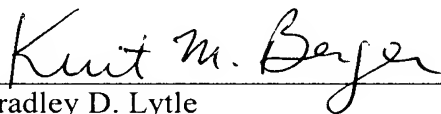
The present amendment also sets forth new Claims 14-27 for examination on the merits. New Claims 14-27 are supported by the originally filed specification and do not add new matter.<sup>4</sup> For reasons similar to those recited above for Claim 1, Applicants respectfully submit that new Claims 14-27 patentably define over the '090 patent.

Thus, it is respectfully submitted that independent Claims 1, 7, 13, 14, 17, 18, 21, 24, and 25 (and all associated dependent claims) patentably define over the '090 patent.

Consequently, in view of the present amendment and in light of the above discussion, the outstanding grounds for rejection are believed to have been overcome. The application as amended herewith is believed to be in condition for formal allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, L.L.P.



Bradley D. Lytle  
Attorney of Record  
Registration No. 40,073

Customer Number  
**22850**

Tel: (703) 413-3000  
Fax: (703) 413 -2220  
(OSMMN 08/09)

Kurt M. Berger, Ph.D.  
Registration No. 51,461

2094368\_1

---

<sup>4</sup> See, e.g., Figures 1, 2B, 15, and 16 and the discussion related thereto in the specification.